



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/384,158	08/27/1999	MICHAEL S. BORELLA	99.226	7444

20306 7590 05/24/2005

MCDONNELL BOEHNEN HULBERT & BERGHOFF LLP
300 S. WACKER DRIVE
32ND FLOOR
CHICAGO, IL 60606

EXAMINER

NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/384,158

Applicant(s)

BORELLA ET AL.

Examiner

Abdulhakim Nobahar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 March 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' amendment received on March 10, 2005.
2. Amendments to claims 1, 10 and 20 are acknowledged and that do not introduce any new matter.
3. Applicants' arguments have been fully considered but they are not persuasive.
4. Applicants on page 8, 2nd paragraph of the remarks argue that "Minear does not disclose a secure communication channel, however, between an internal network device and an external network device that are connected via a router/gateway."

It should be noted that none of the claims of the instant application explicitly recite the existence or establishment of a secure communication channel between an internal network device and an external network device as recited above. However, Minear discloses the use of IPSEC protocol for providing a secure communication (see col. 4, lines 5-45). According to the RFC 1825 and RFC's 1826-1829, IPSEC protocol is designed to provide cryptographic authentication and confidentiality of traffic between two communicating network entities. IPSEC can be used in an en-to-end mode between two communicating nodes or hosts, or in tunnel mode between firewalls or routers, or combination of router/firewall and a workstation. Thus, using IPSEC protocol inherently

enables a system to have a secure communication channel between any two desired communicating nodes.

5. Applicants on page 8, 3rd paragraph of the remarks argue that "Contrary to the Examiner's assertion, Minear does not establish a security association between the first network device and a third network device on a second network external to the first network."

Minear discloses that the sending firewall (corresponding to the recited a second device on a first network) uses the sending userid (the sender corresponds to the recited the first network device) and destination address (the destination device corresponds to the recited a third network device on a second network) to select an appropriate security association (see col. 4, lines 30-35). This function by the sending firewall is the establishment of a security association between the first network device and a third network device that are located on two different networks.

6. In light of the above submission the previous claim rejection under 35 USC § 102 is maintained while taken into account the amendments to claims 1, 10 and 20 as follows.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Minear et al (5,983,350) (hereinafter Minear).

Referring to claims 1-3, Minear discloses a method and system for a secure network by regulating the flow of messages through a firewall and authenticating the sender of a message (col. 2, lines 50-67). Minear further discloses:

“providing a first network device and a second network device on a first network”.

See Figs. 1, 3 and 5, where the workstation H1 and the gateway firewall SW1 correspond to the recited first and second devices on the first network.

“establishing a security association between the first network device and a third network device on a second network external to the first network, the second network device being positioned between the first network device and the third network device”.

See col. 4, lines 8-46; Figs. 1 and 3, where the sending firewall 14 is positioned between the internal device and an external device.

"Specifying an external address of the third network device for the security association". See col. 4, lines 8-28, where the destination address corresponds to the external address...

"Storing the external address in a table on the second network". See col. 7, lines 23-40.

"Mapping at least one of an internal address and a security value to the external address in the table". See col. 4, lines 1-15; col. 5, lines 29-36, where selecting the SPI value based on the destination address and the sender ID corresponds to the recited mapping... and the security association is kept in a table in the firewall (col. 7, lines 23-40).

Referring to claim 4, Minear discloses:

"the security value is a security parameter index for an internet Protocol security protocol. See col. 4, lines 8-12.

Referring to claim 5, Minear discloses:

"the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange protocol. See col. 2, lines 1-5.

Referring to claim 6, Minear discloses:

"specifying the external address of the third network device for the security association with a Port Allocation Protocol external address validating message sent from the first network device to the second network device". See col. 4, lines 8-15 and col. 5, lines 34-45.

Referring to claim 7, Minear discloses:

" the Port Allocation Protocol external address validating message has a valid external address field". See col. 2, lines 27-44; col. 4, lines 24-27; col. 9, lines 27-40 and lines 52-62.

Referring to claim 8, Minear discloses:

"removing the external address from the table with a Port Allocation Protocol external address invalidating message sent from the first network device to the second network device". See col. 5, lines 26-33; col. 9, lines 58-62 and Fig. 3.

Referring to claim 9, Minear discloses:

"the Port Allocation Protocol external address invalidating message has an invalid external address field". See col. 4, lines 24-27; col. 5, lines 26-33.

Referring to claims 10-12, Minear discloses:

"providing a first network device and a second network device on a first network, and a third network device on a second network external to the first network, the second

network device being positioned between the first network device and the third network device". See Figs. 1, 3 and 5, where the workstation H1 and the gateway firewall SW1 correspond to the recited first and second devices on the first network and H2 corresponds to the recited third device on the network. The sending firewall 14 is positioned between the internal device and an external device.

"Sending a packet having an external address from the third network device to the first network device". See Fig. 3, where the H2 device has an address.

"intercepting the packet with the second network device". See Fig. 3, where the packets are processed (corresponding to the recited intercepting) by the gateway firewall SW1 coming from the external network.19.

"determining whether the security value of the packet has been allocated to the first network device". See col. 4, lines 29-42, where identifying a security association based on the destination address (destination address here corresponds to the address of the recited first network device) corresponds to determining...; col. 4, line 59-col. 5, line 8 and col. 5, line 65-col. 6, line13.

"determining whether the external address of the packet has been specified by the first network device as being valid". See col. 5, lines 25-33; col. 5, line 65-col. 6, line13.

"sending the packet from the second network device to the first network device if the security value has been allocated to the first network device and the external address of the packet has been specified by the first network device as valid". See col. 5, lines 9-33.

Referring to claim 13, Minear discloses:

“the security value is a security parameter index for an Internet Protocol security protocol. See col. 4, lines 8-12.

Referring to claim 14, Minear discloses:

“the Internet Protocol security protocol is either an Authentication Header protocol or an Encapsulated Security Payload protocol. See col. 2, lines 1-5.

Referring to claim 15, Minear discloses:

“discarding the packet if the security value of the packet has not been allocated to the first network device”. See col. 5, lines 9-33.

Referring to claim 16, Minear discloses:

“discarding the packet if the external address of the packet has not been specified by the first network device as being valid”. See col. 5, lines 9-33.

Referring to claim 17, Minear discloses:

“discarding the packet if the security value of the packet has not been allocated to the first network device, and discarding the packet if the external address of the packet has not been specified by the first network device as being valid. See col. 5, lines 9-33.

Referring to claim 18, Minear discloses:

" specifying the external address as being valid if a security association has been established between the first network device and the third network device". See col. 4, line 59-col. 5, line 8.

Referring to claim 19, Minear discloses:

"storing a valid external address in a table on the second network device. See col. 7, lines 23-39.

Referring to claim 20, Minear discloses:

"a routing network device using distributed network address translation with security to provide routing services for a plurality of internal and external network devices, the routing network device being positioned between an internal network device and an external network device" (See Fig. 3, where SW1 corresponds to the recited routing network device and it is positioned between the internal device and an external device. col. Col. 4, line 8-45; col. 5, lines 25-45); and

"an established security association table associated with the routing network device for storing external addresses of external network devices that have established security associations with internal network devices" (See Fig. 4, where the security association database 54 corresponds to the recited table and col. 7, lines 23-50), and "mapping external addresses that have been specified as valid by the internal network devices to one of internal network addresses and security values for established security associations" (See col. 4, lines 1-15; col. 5, lines 29-36; col. 7, lines 23-40,

where selecting the SPI value based on the destination address and the sender ID corresponds to the recited mapping... and the security association is kept in a table in the firewall).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Abdulahkim Nobahar
Examiner
Art Unit 2132

AN *a.n.*
May 19, 2005

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100